Information Technology Security Policy

in Washington State Government

Revised November 1997
May 1993

Prepared by:
Washington State
Department of Information Services
PO Box 42445
Olympia, WA 98504-2445
Adopted by:
Washington State
Information Services Board

Information Technology Security Policy
TABLE OF CONTENTS

Policy

Purpose

It is the intent of the Information Services Board (ISB) that state agencies will: (1) develop, implement, maintain, and test IT security plans; (2) train their employees to follow security procedures and standards; and (3) take the steps needed to protect voice, video and computer data, hardware, software, facilities, and personnel. Each agency must be able to demonstrate the ability to comply with this policy.

For purposes of this policy, the IT Security Plan includes the documentation, policies, and procedures that are required to safeguard data, computing and telecommunications facilities, including telephones, hardware, software, and personnel against security breaches.

The principal priorities of IT security are:

1. To maintain data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data;

2. To prevent misuse of, damage to, or loss of IT hardware, software, and facilities;

3. To maintain employee accountability for protection of IT assets; and

4. To prevent unauthorized use or reproduction of copyrighted material.

Scope

This policy applies to all state agencies that operate, manage, or use IT services or equipment to support critical business functions.

The scope includes:

1. Agencies that operate, manage, or use stand-alone, shared, or network-attached computers; whether mainframes, mid-range, or microcomputers for their own use or for use by other agencies;

2. Agencies that operate, manage, or use voice, data, or video telecommunications equipment, networks, or services for their own use or for use by other agencies; and

3. Agencies that purchase computer services or telecommunications network services from other state agencies or commercial concerns.

Policy Statements

It is the policy of the state of Washington that:

Agencies Shall Develop IT Security Plans

Each agency using data, voice, video telecommunications, or computer services for carrying out its mission must develop an IT security plan. Each agency is responsible and accountable for its own IT security plan. Agencies that purchase computer services or telecommunications services from other state agencies or commercial concerns shall integrate their IT security plans to include off-site storage of data with service providers.

Agencies Shall Document IT Security Plans

Agencies shall document their IT security plans in accordance with standards provided by this policy.

Agencies Shall Maintain IT Security Plans

Agencies shall update their IT security plans at least annually and following any significant change to their business, computing, or telecommunications environment. Agency directors shall review and approve the updated plan.

Agencies Shall Validate Security Readiness

Agencies are required to test or validate their security plans and procedures at least once a year. The testing or validation methodology adopted by an agency will depend on:

1. Criticalness of agency business functions;

2. Cost of executing the test plan;

3. Complexity of information systems and components; and

4. Complexity of telecommunications systems and components.

Agencies shall prepare a report documenting their test plans, the results achieved, and recommendations to correct material deficiencies revealed by the test. Agency directors shall review and approve the test report.

Agencies Shall Train Employees to Execute IT Security Procedures

Agencies shall make their employees aware of the need for IT security. Agencies shall train their employees to perform the security procedures required of them.

State Auditor May Audit IT Security Plans

The State Auditor may audit agency IT security plans pursuant to RCW 43.88.160 for compliance with the specified standards.

Effective Date

Effective date of this policy and related standards is June 30, 1994, and as revised on November 1, 1997.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to the standards adopted under this policy. The Department of Information Services (DIS) is responsible for routine maintenance of the standards to keep them current; only major policy shifts require ISB approval**.**

Statutory Authority

RCW 43.105.041 (a) empowers ISB "To develop statewide or interagency technical policies, standards, and procedures . . . ." RCW 43.105.041 (g) empowers ISB "To establish policies for the periodic review by the department [DIS] of agency performance which may include, but are not limited to, analysis of: (a) planning, management, control, and use of information services…"

Standard

The IT security plan for an agency shall provide all applicable information required by this standard.

All state agencies and educational institutions using or providing computer, voice, data, or video telecommunications services must prepare IT security plans. Included are:

1. Agencies with their own computer or telecommunications facilities;

2. Agencies that provide computer or telecommunications services to others; and

3. Agencies using computer or telecommunications services supplied by providers external to their organization.

Each agency is responsible and accountable for its own IT security plan. Agencies using external services shall integrate their IT security plans with service providers.

The IT security plan is primarily for agency use. Agencies may adapt this standard to meet individual needs, but all applicable elements of the standard must be included in the plan. The amount of detail

included in the security plan and the security measures should be commensurate with the size, complexity, and potential business exposure of the installation. An IT security plan must contain enough information to enable agency management to ensure the agency's ability to protect the integrity, availability, and confidentiality of agency information and to protect IT assets from unauthorized use or modification and from accidental or intentional damage or destruction.

An IT security plan may contain references to another organization's IT security plan or to an agency's internal policy, standards, or procedures manual. The agency shall, upon request, make referenced material available for review or audit.

Agencies shall review, evaluate, and update their IT security plan annually or more frequently if appropriate. Agencies must update the plan whenever agency business, computer, or telecommunications environments undergo significant change. Such change may include modifications to: physical facility, computer hardware/software, telecommunications hardware/software, telecommunications networks, application systems, organization, or budget.

If an agency purchases IT services from another organization, the agency and the service provider will work together to make certain the IT security plan for the service provider fits with the agency's plan. If two or more agencies participate with each other in operating an information service facility, then the agencies must develop a joint IT security plan which meets their mutual needs.

Overview

Describe the purpose and organization of the plan. State procedures for updating and distributing the plan. Describe the process for periodic (at least annual) evaluation of the plan and the IT security preparedness of the agency.

Business Impact Analysis

Document the operational, legal, and financial impact that could result from a disruption affecting any computer or telecommunication IT resource of the agency.

Risk, Threat, and Vulnerability Analysis

Document the threats that could result in accidental or intentional disclosure to unauthorized persons or unauthorized modifications, use or destruction of data, computer, or telecommunications resources. Determine the probability of occurrence of each identified threat. Determine the vulnerabilities of IT resources to potential threats. Estimate the loss potential of business areas, either by quantitative or qualitative means. If a risk, threat, and vulnerability analysis was accomplished in the course of developing a disaster recovery/business resumption plan, a summary of the conclusions from that analysis should be included here. This analysis and the business impact analysis should lead to an identification of the principal security exposures of the agency.

Security Strategy

Document the general security strategy of the agency. There are different levels or degrees of security required resulting from the criticalness of data, business application, and IT equipment. Protective measures should be workable and cost effective and aim at preventing the principal security exposures of the agency. The security strategy is an overview of the process that the organization has adopted to protect its data and IT assets.

Personnel Security Practices

Document the general personnel security practices of the agency as they relate to:

1. Hiring practices;
2. Reference checks;
3. Security awareness training;
4. Employee performance requirements; and
5. Vendor and service personnel monitoring.

Physical Security

Establish physical security controls over large computer, minicomputer, and microcomputer equipment consistent with the criticalness of the equipment. Document the physical security standards in the agency as they relate to:

1. Facility characteristics;
2. Access control;
3. Fire and water control;
4. Electrical control;
5. Operational stability;
6. Data storage and telecommunications controls;
7. Off-site storage and environmental controls; and
8. Insurance coverage for computer operations.

Data Security

A. Establish data security controls over large computer, minicomputer, and microcomputer-based data consistent with the criticalness of the data processed. Document the data security standards in the agency as they relate to:

1. Agency data security policy statement;
2. Storage of back-up copies of critical files, documentation, and forms;
3. Monitoring distribution of output reports and introduction or release of data;
4. Data entry processes;
5. Processing accuracy;
6. Processing audit trails;
7. Access control techniques;
8. Terminal, remote job entry (RJE) or network node access security;
9. System access violations;
10. Controls to prevent unauthorized use or removal of tape files, diskettes, and other media; and
11. Controls to prevent the introduction of unauthorized programs into computer systems.

Telecommunications Operational and Physical Security

Establish telecommunications security controls over large computer, minicomputer, and microcomputer-based systems consistent with the criticalness of the data processed. Document the telecommunications security standards in the agency as they relate to:

1. Management of the telecommunications management function and establishment of standards and procedures;
2. Documentation and control of telecommunications equipment inventories, changes, and locations;
3. Location of communications equipment; and
4. Prevention of tampering.

Access Security

Establish access security controls over large computer, minicomputer, and microcomputer-based systems consistent with the criticalness of the data processed. Document the access security standards in the agency as they relate to:

1. Access control;
2. Recording of telecommunications accesses;
3. Control of the use of dial-up lines; and
4. Monitoring of manufacturer, software vendor, and third-party access lines to the computer system.

Protection of Software and Other Copyrighted Material

Document the agency policy on protection of copyrighted material. Require employees to comply with copyright laws.

Plan Evaluation

Document the IT Security Plan Evaluation program. Specify necessary checks or tests and assign responsibility for overseeing them. State the purposes for conducting evaluations of the security plan. Include the policies and guidelines that will apply to evaluation of the security plan. Formulate a test schedule. For each test, specify the detail of the test, the scope or areas to test, and the frequency or target date of the test. Include a brief report describing findings for each completed security check or test and the recommended action.

Training for IT Security

Specify the aims, training activities, schedule, and administrator for agency IT security training. Describe regularly occurring training activities. Employee training should cover the following concepts:

1. Preventing unauthorized access to, damage to, misuse of, or loss of IT hardware, software, data, and facilities;
2. Employee accountability for protection of IT assets;
3. The use or reproduction of copyrighted material; and
4. Periodic evaluation of the plan.

Plan Maintenance

Assign plan maintenance responsibility. Provide a schedule for regular, systematic review of the content of the IT security plan. Document the procedure used for making changes to the plan. Provide policies and procedures for distributing the IT security plan and updates to the plan. The IT security plan may contain sensitive information about the agency's business, communications, and computing operations. Policy and procedures for distribution of the plan should consider sensitive information. Such information should be shared only with personnel who have a need to know.

Guidelines

The purpose of this guideline is to provide an example of tips and techniques for implementing the IT Security Plan. This guideline is not intended to present the only acceptable method for achieving security. An agency may elect to use alternate methodology or adapt this guideline to their specific environment and requirements.

This guideline is organized in the security plan format specified in the IT Security Plan Standard. The amount of detail included in the security plan and the security measures should be commensurate with the size and complexity of the installation. In general, the emphasis should be on data, network, and physical security. Unauthorized or improper access to hardware, network, data, or programs at either the remote site or host computer could result in substantial harm. Therefore, much of the material in this guideline should be considered.

Overview

Describe the purpose and organization of the plan. State procedures for updating and distributing the plan. Describe the process for periodic (at least annual) evaluation of the plan and the IT security preparedness of the agency.

Business Impact Analysis

If a business impact analysis was accomplished in the course of developing a disaster recovery/business resumption plan, a summary of the conclusions from that analysis should be included here. The business impact analysis and the risk, threat, and vulnerability analysis should lead to an identification of the principal security exposures of the agency.

1. Establish an understanding of the business organization and IT resources of the agency.

    a. Identify the business functions to be addressed in accomplishing a business impact analysis;

    b. Identify essential business functions; and

    c. Develop an understanding of IT resources and interdependencies of the essential functions identified.

    Essential business functions are those functions that must take place in order to support an acceptable level of business continuity for the agency.

2. Establish the priorities of senior agency management. There are three major tasks in this procedure:

    a. Identify key senior management personnel;

    b. Schedule and conduct interviews; and

    c. Summarize continuity concerns and priorities.

3. Document the operational and financial impact that could result from exploiting a security exposure of the business area of the agency. There are four tasks in this procedure:

    a. Gather operational and financial impact data;

    b. Develop security exposure scenarios;

    c. Analyze operational impact; and

    d. Analyze economic impact.

4. Criteria for establishing the criticalness of business functions:

    The key principal involved is that only those functions that must be performed, because they are key to the continuation of the organization, should be listed as a top priority. The following criteria are some suggested for determining the criticalness of business functions:

    a. Maintenance of public health and safety;

    b. Income maintenance for citizens;

    c. Income maintenance for government employees;

    d. Payments to vendors for goods and services;

    e. Requirements for compliance or regulation;

    f. Effect on state government cash flow;

    g. Recovery costs;

    h. Effect on production and delivery of services;

    i. Volume of activity;

    j. Effect on public image; and

    k. Inter-system dependency.

Risk, Threat, and Vulnerability Analysis

Document the threats that could result in accidental or intentional disclosure to unauthorized persons, or unauthorized modification, use, or destruction of data, computer, or telecommunication resources. Determine the probability of occurrence of each identified threat. Determine the vulnerabilities of IT resources to potential threats. Estimate the loss potential of the service area, either by quantitative or qualitative means. If a risk, threat, and vulnerability analysis was accomplished in the course of developing a disaster recovery/business resumption plan, a summary of the conclusions from that analysis should be included here. This analysis and the business impact analysis should lead to an identification of the principal security exposures of the agency.

1. Document the threats that could result in accidental or intentional disclosure to unauthorized persons, or result in unauthorized modifications, or use or destruction of data, computer, or telecommunications resources.

   There are many natural and manmade threats to IT resources that could cause business interruption. Potential threats to consider include personnel, physical environment, hardware/software systems, telecommunications, applications, and operations.

2. Threats affecting security planning:

   Intentional Acts

   a. Alteration of data;

   b. Alteration of software;

   c. Bomb threat;

   d. Computer viruses and other malicious code;

   e. Disclosure of confidential information;

   f. Electronic emanations;

   g. Employee sabotage;

   h. External sabotage;

   i. Fraud;

   j. Hackers;

   k. Riot/civil disturbance;

   l. Strike;

m. Terrorist activity;

n. Theft;

o. Unauthorized use; and

p. Vandalism.

Accidents

a. Employee errors, accidents, and omissions;

b. Disclosure of confidential information;

c. Electrical disturbance;

d. Electrical interruption; and

e. Spill of toxic chemical

Physical or Environmental Threats and Failures

a. Fire damage;

b. Water damage;

c. Electrical outages and fluctuations;

d. Structural failure;

e. Hardware failure;

f. Liquid leakage;

g. Operator/user error;

h. Software error; and

i. Telecommunications interruption.

Natural Hazards

a. Earthquake;

b. Flooding;

c. Landslide;

d. Lightning;

e. Sandstorm or blowing dust;

f. Snow and/or ice storm;

g. Tornado;

h. Tsunami;

i. Volcanic eruption;

j. Smoke, dirt, and dust; and

k. Windstorm.

3. Determine the probability of occurrence of an identified threat.

   Many potential threats occur regularly. Regularly occurring threats, historical occurrences, and statistical probabilities are maintained by organizations such as the Federal Emergency Management Agency (FEMA), the Federal Communications Commission (FCC), and the U.S. Fire Administration. Statistics on naturally occurring disasters, burglaries, power outages, fires and storms are usually available from local, state, or federal agencies.

   Local threats to IT resources, such as hardware failures and unauthorized data access attempts are usually logged in the organization's problem tracking system or management status reports.

4. Factors affecting threat occurrence rate:

   a. Geographical location;

   b. Facility environment;

   c. Data sensitivity/criticalness;

   d. Protection and detection features;

   e. Visibility;

   f. Proficiency level;

   g. Security awareness;

   h. Emergency training;

   i. Staff morale;

   j. Local economic conditions;

k. Redundancy of control;

l. Availability and use of written operating and security procedures;

m. Compliance level (measure of the level of observance or enforcement of security procedures); and

n. Past prosecutions.

5. Determine the vulnerabilities of IT resources to potential threats.

   Vulnerability to a specific event is created when an agency is open to abuse or misuse or subject to indiscriminate use. Vulnerability may be measured by the cost an agency would incur if that event took place.

   For many threats, the vulnerability to a business can be mitigated with controls. For example, vulnerability to data storage and retrieval in a distributed database can be partially mitigated through controls that ensure verification that the receiver of the transmission is the intended site and not an intruder, prevention of intruders from intercepting messages, and consistent allocation of authorization rules at the distributed database sites. Vulnerability considerations include natural disasters, environment, facility housing, access, work scene, and data value.

6. Typical vulnerabilities to consider:

   a. Operating system flaws;

   b. Inadequate audit/security mechanism;

   c. Power supply;

   d. Building construction;

   e. Access control;

   f. Fire protection;

   g. Operating procedures;

   h. Supply and service procedures;

   i. Emergency procedures;

   j. Security procedures and security officer;

   k. Management policies and procedures;

   l. Personnel policies and procedures; and

m. Communications architecture.

7. Estimate the loss potential of a service area, either by quantitative or qualitative means.

   The impact of an event is the amount of damage it could cause. The frequency of occurrence of that event is the number of times it could happen. If these two numbers are precisely known, the product of the two would be a statement of loss, that is, Loss = Impact X Frequency of Occurrence. Since the exact impact and frequency usually cannot be specified, it is only possible to approximate the loss with an annual loss exposure (ALE). The ALE is the product of estimated impact and estimated frequency of occurrence per year. This method is the quantitative approach to analyzing loss potential.

   In the qualitative approach, the probability and impact of an event are estimated in orders-of-magnitude i.e.; qualitative terms such as low, medium, or high.

Security Strategy

Document the general security strategy of the agency. There are different levels or degrees of security resulting from the criticalness of the data, business area, and IT equipment. Protective measures should be workable and cost effective and aim at preventing the principal security exposures of the agency. The security strategy is an overview of the process that the organization has adopted to protect its data and IT assets.

1. Establish security policies for both information systems personnel and users of computer services.

   a. Policies should emphasize agency guidance covering the importance of preventing unauthorized access, misuse, damage to, or loss of IT hardware, software, data and facilities. Policies should include statement of actions to be taken for failure to observe security rules and procedures.

2. Assign responsibility for IT security to an individual or group that can administer the function independently.

   a. Specify physical security arrangements and controls for operations that are appropriate given the size and purposes of the installation; and

   b. Determine that the function responsible for IT security has proper authority to install, monitor, and enforce security rules and procedures.

Personnel Security Practices

Develop, document, and implement security standards and procedures for employee or contractor selection, orientation, and supervision. The objective is to ensure that a high level of integrity and satisfactory staff conduct is achieved and maintained, and to promote an awareness of security matters. The following should be included:

1. Hiring practices.

   Define acceptable levels of prior performance consistent with the sensitivity of the planned work assignment. Consider checks with former peers and/or supervisors at places of prior employment, as well as with references provided.

2. Reference checks.

   Reference checks that include education and previous employment may be considered for selected personnel who will be required by their job to have access to sensitive information.

3. Security awareness training.

   Develop a formal security orientation and training program for all employees. The program should be current and comprehensive. It should deal with:

   a. Applicable laws and/or rules;

   b. Applicable state policies and standards; and

   c. Agency security policies, plans, and procedures.

4. Employee performance requirements.

   a. Provide specific supervision for new employees working in sensitive areas or on sensitive processes; and

   b. Ensure appropriate separation of responsibility and adequate audit trails in sensitive functions.

5. Vendor and service personnel monitoring.

   a. Establish procedures for orientation and monitoring of the activities of contractors and service personnel.

Physical Security

Data processing and agency management are responsible for assuring that adequate protective measures are implemented for large computer, minicomputer, and microcomputer resources even though the construction or modification of the facility may be the responsibility of the Department of General Administration, the Institution Facility Department, or a private landlord.

1. Facility characteristics.

   Where justified, the physical facility should be constructed in accordance with the standards specified in the current National Fire Protection Association (NFPA) publication No. 75, "Protection of Electronic Computing/Data Processing Equipment."

2. Location and layout of the facility.

   a. Locate large (mainframe) computer equipment in a secure, environmentally controlled facility;

   b. If the computer facility is located in a multi-floor facility, assess the risk of damage from plumbing failures, equipment, or occupants of upper floors;

   c. Locate the computer facility inconspicuously with no references or direction signs;

   d. The general location of the computer room within the overall facility should be outside heavy traffic patterns;

   e. Locate mini and/or microcomputer IT resources in an area of authorized traffic;

   f. Locate mini and/or microcomputer IT resources in a facility that can be locked during non-prime shift hours, if the criticalness of the resources require such precaution;

   g. Use asset tags or other identification markings for all computer equipment; and

   h. Compare accounting department fixed asset records of computer equipment and the actual physical equipment on an annual basis.

3. Large computer (mainframe) room physical security attributes to consider.

   a. The existence of locking mechanisms to limit computer room access to authorized individuals;

   b. The placement of computer room outside walls and any windows to limit access to unauthorized individuals;

   c. The general structure of interior walls to determine that they are secure and are constructed from floor to true, not false, ceiling;

d. The location of power transformers and air-conditioning units to provide proper protection;

e. Fire detection equipment including zone-controlled heat and smoke detectors;

f. An overall fire protection system including a zone-controlled system and local extinguishers;

g. The location of air-conditioning units and power transformers to determine that they are properly protected;

h. Back-up power generation and Uninterruptable Power Supply (UPS) equipment including the rated capacities;

i. Adequate computer room temperature, humidity, and other environmental controls;

j. Regular inspection and maintenance of physical and environmental controls;

k. Temperature and humidity controls in place and a method to assess the adequacy of procedures for monitoring those controls;

l. Power controls;

m. Construction fire codes;

n. Sensitive and/or negotiable material; and

(1) Expensive assets such as computer equipment; and

(2) Devices providing access to sensitive data.

o. Perimeter security for surrounding areas.

4. Access control.

    a. Identify critical areas and designate specific personnel who require access to these areas;

    b. Limit access to the computer operations facility to authorized persons;

    c. Arrange for positive identification using pass, key lock, badge system, cipher lock, or other controls for employees, suppliers, and visitors to access the computer room;

    d. Change locks or lock combinations to the computer room on a periodic basis;

    e. Establish a control system to ensure identification of the individuals having possession of the keys, cards, and badges at any given time;

    f. Frequently review the list of assigned key cards or access rights and determine that all persons on the list are still authorized employees;

    g. Use logs or special badges for visitors to the computer room;

    h. Control access of maintenance and other facilities personnel to the computer room;

    i. Require managers to frequently visit the computer room facility on an unannounced basis during a non-prime shift and determine that access control procedures are being followed;

    j. Consider establishing a system for the control of packages or containers entering or leaving the restricted area;

    k. When an employee is terminated, immediately escort the terminated employee from the computer room and cancel that employee's access rights;

    l. Equip any supplementary doors within the computer room facility with exit only locks and audible alarms.;

    m. Provide for prompt reporting of any actual or suspected hostile act to the appropriate security or law enforcement agency;

    n. Use locking devices to secure critical freestanding mini/microcomputer systems;

    o. Use locks to secure the chassis of critical mini/microcomputer system from improper removal of boards and from unauthorized operation, whether or not the system is attached to its work platform; and

    p. Ensure that critical mini/microcomputer workstations are properly locked, that work areas are clear of programs and diskettes, and that locking keys are properly secured during off-shift hours.

5. Fire and water control.

   Install appropriate controls in the computer operations facility to protect equipment, materials, and employees against fire or water hazards.

   a. Fire prevention/detection/suppression measures should be implemented in accordance with the standards specified in the current National Fire Protection Association (NFPA) publication No. 75, "Protection of Electronic Computing/Data Processing Equipment";

   b. Protect the computer facility with zone controlled smoke and fire detection equipment, both above and below the raised floor, and ensure that activation of these devices will result in an audible alarm in the computer room, as well as automatic notification of the nearest fire department;

   c. Equip the computer room with an overall, zone controlled fire control system, as well as appropriate portable extinguishers;

   d. Locate master power switches at each major door to the computer room;

   e. Post fire evacuation charts prominently, and conduct evacuation drills on a periodic basis;

   f. Equip the computer room facility with flame retardant, waterproof plastic covers for placement over major data processing equipment items;

   g. Ensure that the computer facility is inspected periodically by local fire inspectors and identify actions taken to correct any findings indicated on their last report;

   h. Use flame resistant materials for floor and ceiling tiles, and construct ductwork to minimize the risk of fire;

   i. Water supply and drainage systems should be designed to preclude damage from bursting pipes or standing water;

   j. Install drains under the raised floor to help avoid water accumulation in the event of flooding; and

   k. Establish procedures for an orderly shutdown of computer facilities in the event of flooding or a major weather disturbance.

6. Electrical control.

   a. The electric utility should provide a stable power supply with alternate routing when possible. Investigate the feasibility of Uninterruptable Power Supply (UPS) systems for critical devices;

   b. All electrical appliances (as a single unit), including computers, must be approved by a recognized testing lab, but not necessarily Underwriter's Laboratory. (Refer to WAC 296-24-95601.) ; and

c. Install electrical line surge protectors on all mini and/or microcomputer systems.

7. Operational stability.

   a. Develop and implement measures to ensure operational stability;

   b. Establish procedures to identify and document problems and to facilitate their resolution. Include the following:

      (1) Problem logging;

      (2) Resolution monitoring;

      (3) Cause/solution analysis; and

      (4) Procedures for corrective action.

   c. Establish procedures to record equipment failures and to maintain equipment on a regular and emergency basis:

      (1) Establish manual and automated logging procedures for recording equipment failures;

      (2) Establish procedures to obtain appropriate levels of approvals for calling in maintenance personnel during all operating shifts;

      (3) Log and report on-line remote maintenance used for hardware or software problems; and

      (4) Perform equipment maintenance on a regular basis consistent with equipment requirements.

   d. Define and implement staff technical training programs to ensure operational stability; and

   e. Provide for control and maintenance of operational, systems, and program documentation.

8. Data storage and telecommunications controls areas.

   a. Establish access, fire, and other controls for the prime data storage facility that are appropriate and consistent with procedures used in the main computer room facility;

   b. Establish procedures for logging data in and out of the media library;

   c. Establish access, fire, and other controls for the telecommunications control area which are appropriate and consistent with other computer room procedures; and

   d. Ensure that cabling of telephone or local network lines from remote devices to the telecommunications facility are shielded or obscured from view.

9. Ensure that the off-site media storage location's security and environmental controls are adequate.

    a. Ensure that media storage meets needs for archival and/or rotational access;

    b. Ensure that storage of paper media, magnetic media, or both, is allowed;

    c. Ensure that media storage area meets agency needs for common vaulting, safe-deposit boxes, and/or electronic vaulting;

    d. Ensure that storage security needs will be satisfied through use of guards, TV monitors, third-party surveillance, and/or automated security systems; and

    e. Ensure that storage building environment provides adequate protection from fire, electrical problems, civil disturbance, and natural disasters.

10. Insurance coverage for computer operations.

    a. The agency may wish to consider insurance coverage for data processing equipment and media including:

        (1) Losses from fire, earthquake, or flood damage;

        (2) Losses from equipment breakdowns such as sprinkler system leakage;

        (3) Losses from theft or vandalism; and

        (4) Losses from civil commotion or riot.

    b. The agency may also wish to consider insurance coverage for business interruptions, given the organization's dependence upon key computer applications.

Data Security

Establish data security controls over large computer, minicomputer, and microcomputer-based data consistent with the criticalness, confidentiality, and privacy needs of the data processed. Consider security needs when data is shared by multiple agencies.

1. Agency Data Security Policy Statement

   Publish and distribute a data security policy statement addressing such subjects as:

   a. Ownership, custodial, and user information security responsibilities;

   b. Protection of copyrighted material;

   c. Automated information access control; and

   d. Data and program back-up:

      (1) Specification of data and programs that require no back-up;

      (2) Specification of data and programs that require a secure on-site back-up; and

      (3) Specification of data and programs that require both on-site and off-site back-up.

2. Storage of back-up copies of critical files, documentation, and forms.

   Store back-up copies of critical files, documentation, and forms in a secure, off-site location.

   a. Identify critical systems records to be stored at off-site storage locations. Determine what records will be needed to restore service for various levels of system failure. Establish procedures for the creation, maintenance, verification, and emergency use of back-up data. The following should be considered:

      (1) Data files that include magnetic tape master files, disk dumps, and transaction files;

      (2) Application programs;

      (3) Job control language;

      (4) Systems software, including custom software;

      (5) Program and systems documentation;

      (6) Operational documentation; and

      (7) Security, back-up, and recovery procedures.

b. Establish a data classification system so that each data file can be categorized in accordance with the sensitivity and criticalness of the information contained;

c. Periodically select several key applications and determine that key versions of data files as well as documentation and special forms are stored in the off-site location; and

d. Establish an inventory listing of all items in the off-site location and keep it current.

3. Distribution of output reports and introduction or release of data.

   Monitor the distribution of output reports as well as the introduction or release of data and program files.

   a. If users pick up output reports from the computer operations facility, ensure that only authorized persons may pick up their reports;

   b. If an office courier or mail distribution system is used for output report distribution, establish procedures to ensure that reports go only to appropriate recipients and that confidential reports are sealed;

   c. Establish procedures for the production and distribution of key documents such as payroll checks;

   d. Provide for authorization, logging, and audit trail for non-routine distribution of system output;

   e. Provide for disposal of unclaimed output;

   f. Establish controls over releasing data files to outside users and ensure that adequate levels of approval are required;

   g. Establish procedures for bringing data and program files into the computer system and control the risk of exposure to computer viruses through the introduction of such files; and

   h. Establish controls covering the import or export of data through any LAN gateways to other computerized systems beyond the LAN, the use of office automation equipment for non-business applications, and the introduction of non-authorized software into the LAN.

4. Data entry processes.

   a. Establish source data entry authorization procedures as appropriate. Include the following:

      (1) Authorization signatures;

      (2) Separation of responsibility for data entry and authorization;

(3) Password and other appropriate security and accounting codes for on-line data entry; and

(4) Operator identification and audit trail.

b. Provide for balance and control procedures.

(1) Batch and/or hash totals;

(2) Check digits; and

(3) Verification.

5. Processing accuracy.

Establish processing accuracy controls:

a. Running file balance totals;

b. Batch totals;

c. Processing cycle transaction counts and dollar or hash totals;

d. Separation of responsibility for operation and control checking; and

e. Sensitive document controls.

6. Processing audit trails.

Establish processing audit trails:

a. Data entry authorization;

b. Operator logging;

c. Processing control and balance reports;

d. Transaction log files; and

e. Output distribution logs.

7. Access control techniques.

Establish policies and procedures for data access:

a. Define user responsibility for data file access and use;

b. Develop access authorization requirements;

(1) Identify sensitive data and specify access rights; and

(2) Establish procedures for authorization for non-routine access and use.

c. Establish password control for access to sensitive data, and establish mandatory password changes on a periodic basis;

d. Use other hardware/software access control features as appropriate;

(1) Database system features;

(2) File and data management capabilities of the operating system;

(3) Data encryption;

(4) Terminal locks/software locks; and

(5) Security access software systems.

e. Ensure that communication lines and controller are adequately protected from damage as well as unauthorized access;

f. Review files that have not been flagged as being password protected and determine whether any should be protected; and

g. Change passwords and user identification codes (IDs) on a regular basis.

8. Terminal, remote job entry (RJE), or network node access security.

a. Physical access controls;

b. Software disable during "off shift"; and

c. Hardware/software restriction based on access need of specific device.

9. Media protection.

Establish procedures for control and disposition of data storage media containing sensitive data.

a. Control and erasure of scratch media;

b. Control of checkpoint/restart data;

c. Control of log or journal files; and

d. Control of media library.

10. System access violations.

    Monitor system access violations for subsequent action and ensure that controls exist to limit such access attempts.

    a. Determine that terminal access codes, menu screens, and personal passwords are changed on a periodic basis;
    (1) Determine that computer system access rights are changed or canceled for individuals who have either terminated employment or changed job responsibilities; and

    b. Assign responsibility and procedures for follow-up to unauthorized access attempts.

11. Controls to prevent unauthorized use or removal of tape files, diskettes, and other media.

    Establish controls over tape files, diskettes, and other media to prevent unauthorized use or removal from IT resource areas.

    a. Establish procedures for storing and controlling tape files, diskettes, or other removable media;

    b. Specify that labels, volume and serial numbers, and other identifiers consistent with the computer operating system are used for all files;

    c. Outline the procedures for implementing retention schedules as outlined by the State Records Committee and the Secretary of State; and

    d. Establish procedures for the disposal of documents containing personally identifiable information.

12. Controls to prevent the introduction of unauthorized programs to computer systems.

    a. Establish procedures for introducing new software to computer systems;

    b. Install virus detection software on computer systems and establish procedures for use of this software;

    c. Establish a procedure to list selected directories of computer program libraries and verify that sampled programs are properly authorized;

    d. Verify that passwords associated with the security software are changed on a periodic basis;

    e. Establish a policy, acknowledged by employees, which prohibits the introduction of unauthorized programs to any computer system; and

    f. Establish policies to control the general downloading of programs from sources such as computer bulletin boards, Intranets and the Internet.

Telecommunications Operational and Physical Security

Management of the telecommunications management function and establishment of standards and procedures.

1. Establish a management function with the authority to establish telecommunication standards and procedures.

2. Establish telecommunication departmental standards for such areas as:

    a. Approved equipment types, such as workstations (terminals, microcomputers, mini-computers), which can be introduced to networks;

    b. Authorization procedures for introducing new equipment to networks;

    c. Schedules and procedures for authorizing the introduction of communication lines, network addresses, and workstations outside normal operating hours;

    d. Procedures for the use of any dial-up data lines;

    e. Determine that there is an appropriate level of management approval for changes to the telecommunications network; and

    f. Communicate the telecommunications network management policies and procedures to users of the network.

3. Documentation and control of telecommunications equipment inventories and equipment changes.

    a. Include all data communications equipment on inventory lists, e.g., modems, controllers, workstations, communication lines, and related devices;

    b. Ensure that only authorized workstations are connected to the network;

    c. Physically verify inventory information by checking the actual workstation installations;

    d. Use network diagrams to document both physical and logical connections between telecommunications and other data processing equipment;

    e. Verify items of telecommunications equipment, wherever located, and trace them to inventory records and to network diagrams to determine that records are accurate;

    f. Ensure that network diagrams are stored in a location protected from unauthorized access;

g Establish procedures for such matters as adding a new workstation or changing a port assignment;

h. Establish a formal testing procedure covering the introduction of any new equipment or changes to the telecommunications network; and

i. Provide for verification that formal testing procedures are followed.

4. Location of communications equipment.

   a. If possible, install communications equipment in a secure locked room with access limited to authorized individuals;

   b. If some communications equipment, such as a communications controller, is kept in the computer operations area, ensure that physical security within that area also is adequate;

   c. Authorize only persons with the responsibility and knowledge to use communications equipment to enter the facility housing that equipment; and

   d. Locate master workstations that can change the access rights of other workstations or users in secure areas only.

5. Prevention of tampering.

   a. Place all lines located in areas near the communications equipment room out of sight;

   b. Where justified by data sensitivity and potential exposure, label communication lines within the equipment room and elsewhere with a code maintained by telecommunications management rather than with a physical description;

   c. In situations where the privacy of data is of great importance, establish procedures requiring the shielding of cables and workstations to prevent electrical emanations which could be intercepted and read by an unauthorized person;

   d. Check the data communications network on a periodic basis for active or passive wiretaps; and

   e. Ensure data packets transmitted through routers, switches and gateways are appropriately filtered.

Access Security

The following controls are suggested for site access control:

1. Control all system access through passwords and authorization codes that are validated by security software.

    a. Require written requests for Logon Ids;

    b. Do not allow the use of shared Logon Ids, unless for authorized and approved business justification or if shared Logon Ids are the only practical solution;

    c. Do not allow concurrent use of Logon Ids;

    d. Cancel workstation access authorizations when a workstation has been inactive for a specified length of time;

    e. Use non-dictionary passwords;

    f. Assign Logon Id's to specific individuals rather than functions or groups of individuals;

    g. Require passwords expire in a maximum of 60 days;

    h. Require passwords be changed as soon as they expire with a limit of one grace logon;

    i. Require passwords have a minimum length of five characters;

    j. Allow owner of Logon Id to change his/her own password;

    k. Require the user at their first logon change all passwords;

    l. Discourage users from displaying or sharing their passwords;

    m. Exclude passwords from batch files;

    n. Require passwords not be reused for a minimum of five iterations;

    o. Establish "intruder lockout" for 24 hours or until LAN Administrator unlocks the ID after five unsuccessful attempts of authentication;

    p. Cancel Logon Id's when an individual leaves the organization or has a change in responsibilities; and

    q. Check personnel records of former employees and determine that their workstation access rights have been deleted.

2. Recording of telecommunications accesses.

    a. Log all telecommunications accesses to the computer system;

    b. Provide for review of computer or telecommunications control logs, and follow-up on exception situations;

    c. Ensure that any exceptions have been reviewed and resolved by appropriate levels of management; and

    d. Develop service level agreements from network service providers to log and support the review of exception situations.

3. Control of the use of dial-up lines.

    a. Control the use of dial-up connections to the computer systems and workstations to prevent unauthorized access attempts;

    b. Identify the dial-up connections that are available within the telecommunications network, determine whether the existing dial-up connections are necessary and have been approved by management;

    c. Ensure that the security system logs all unsuccessful password or authorization code access attempts;

    d. To prevent unauthorized access attempts, in situations where the sensitivity of data is of great importance, install "call back" or "see through" security devices or logical network security passwords on all dial-up connections to the computer system;

    e. To prevent accidental line detection, if possible, assign dial-up access numbers to a three-digit exchange number different from the organization's main telephone exchange;

    f. Establish procedures for authorizing users to access the dial-up system and screen all users prior to authorizing them; and

    g. If possible, and where cost-effective, change dial-up access telephone numbers on a periodic basis.

4. Monitoring of manufacturer, software vendor, and third-party dial-up access lines to the computer system.

    a. Monitor the use of manufacturer, software vendor, and third party dial-up access lines to the computer system. Change access numbers and access codes frequently.

5. Establish policies for using the Internet

    a. Include policies for responsible use, authorization and confidentiality issues for the internal intranet and external Internet.

6. Protect Voice Telecommunication (SCAN) authorization codes for access to long distance dialing.

    a. Establish procedures to prevent disclosure of SCAN authorization codes; and

    b. Do not allow employees to share SCAN authorization codes.

Protection of Software and Other Copyrighted Material

Agency policy on protection of copyrighted material.

1. The state of Washington expects its employees to comply with copyright laws. It is, therefore, important for agencies to have a policy on protecting copyrighted material. Courts have found organizations and their officers liable for copyright infringement where unauthorized copies were used to the organization's benefit - even when the copying was done without management's knowledge;

2. Employees required to comply with copyright laws;

   It is expected that agency policy will notify employees that they are required to comply with copyright laws. The policy should convey that:

   a. Documents or software protected by copyright may only be copied with the written permission of the copyright holder;

   b. Any unauthorized reproduction of the copyrighted material may subject the responsible employee to disciplinary action, civil liability, or both;

   c. The state and/or agency is not obligated to defend or indemnify employees in actions based on copyright violation; and

   d. The agency policy may include statements such as the following suggested by the Software Publishers Association:

      "(Agency) licenses the use of computer software from a variety of outside companies. (Agency) does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.";

      "With regard to use on local area networks or on multiple machines, (Agency) employees shall use the software only in accordance with the license agreement.";

      "(Agency) employees learning of any misuse of software or related documentation within the (Agency) shall notify [Agency management].''; and

      "According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000, and criminal penalties, including fines and imprisonment. (Agency) employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination. (Agency) does not condone the illegal duplication of software."

Plan Evaluation

Document the IT Security Plan Evaluation program. Specify necessary checks or tests and assign responsibility for overseeing them. State the purposes for conducting evaluations of the security plan. Include the policies and guidelines that will apply to evaluation of the security plan. Formulate a test schedule. For each test, specify the level of the test, the scope or areas to test, and the frequency or target date of the test. Include a brief report describing findings for each completed security check or test.

Training for IT Security

Specify the aims, training activities, schedule, and an administrator for agency IT security training. Describe regularly occurring training activities.

Plan Maintenance

Assign plan maintenance responsibility. Provide a schedule for regular, systematic review of the content of the IT security plan. Document the procedure used for making changes to the plan. Provide policies and procedures for distributing the IT security plan and updates to the plan. The IT security plan may contain sensitive information (confidential or private) about the agency's business, communications, and computing operations or employees. Policy and procedures for distribution of the plan should consider sensitive information. Such information should be shared only with personnel who have a need to know.